

New technology advances protection of critical systems from insider-assisted attacks

October 24 2018, by Chris Adam



New technology from Purdue University advances the protection of critical systems from insider-assisted attacks. Credit: Purdue University

Here's a scary yet realistic scenario: Attackers sponsored by a rogue organization or radical state gain access to the control system of a nuclear reactor, a chemical reactor or a similar critical system.

Is the reactor system smart enough to know it is attacked? The answer:

Most experts would tell you if an insider assists attackers, nearly all industrial systems become vulnerable. Worse yet, the system could remain defenseless and sustain physical damage from an attack.

"Security defenses against digital attacks are for the most part based on the concept of erecting walls or fences to stop unauthorized access from outsiders," said Hany Abdel-Khalik, a Purdue University associate professor of nuclear engineering, who is leading the research team.

He said it is similar to building a physical wall, a trench or a line of armed warriors to stop enemy advances.

"When there is a clear barrier, your job is well defined and you will try everything you know until the wall comes down." Abdel-Khalik said.

"Hackers have proven it is possible in the digital world to take down a barrier without operators being aware. There is a clear need for another line of defense when these types of security walls are compromised."

The Purdue team has developed a new covert defense algorithm that employs evasive tactics to deceive attackers. The idea is to modify all the signals flowing through the network, from and to the sensors and plant components, by small amounts that do not impact system behavior but provide the ability to detect intrusion.

Different from a real wall, the attackers do not see their target because the covert signals look like noise normally expected in the system traffic. Operators also can make the covert signals nearly impossible to figure out by continuously changing them.

The Purdue team said the new [defense](#) has applications for many industrial control systems that uses computers to continuously monitor operations and issue commands to maintain safe and economical system operations. These include nuclear plants, refineries, driverless vehicles,

drones and Internet of Things devices.

Provided by Purdue University

Citation: New technology advances protection of critical systems from insider-assisted attacks (2018, October 24) retrieved 3 May 2024 from <https://phys.org/news/2018-10-technology-advances-critical-insider-assisted.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.